KeyLED - Transmitting sensitive data over out-of-band channels in wireless sensor networks

Rodrigo Roman, Javier Lopez
University of Malaga, Spain

September 29th, 2008
WSN Security
Out-of-Band Channels

- Sensor networks are specially vulnerable against external and internal attacks due to their peculiar characteristics
- Focus on attacks to the Information Flow
  - Easy access to the information of an (unprotected) wireless channel
- "Out-of-band" Channels?
  - Limited capabilities
  - Spatial relationship Sender ↔ Receiver
  - (Usually) require the presence of a human user

  1. Devices are near when communication takes place
  2. Difficult to Eavesdrop / Modify information flow
  3. Human user can certify which is the sender & which is the receiver

Applicability?
Feasibility?
I. APPLICABILITY

Wireless Sensor Networks + “Out-of-Band” Channels

- Properties:
  - Two previously unrelated nodes can share sensitive information
  - Assume that the source device is physically near
- QUESTION: ¿IS THIS REALLY USEFUL?
WSN and “Out-of-Band” channels

- **Pre-Deployment Phase** - Configure the nodes
  - ✓ Load the motes with
    - Application-specific information
    - Node-specific sensitive information
  - *When?* Configuring motes on potentially unsafe environments

- **Deployment Phase** - Establish pairwise keys
  - ✗ Not specially useful
    - Scalability
    - Practical reasons
WSN and “Out-of-Band” channels

- **Network Extensibility** - Add new nodes after deployment
  - Establish a pairwise key
    - Send ephemeral key to protect subsequent negotiations
    - Applicable to certain Zigbee configurations (“over-the-air”)
  - Send public information (e.g. Certificates)
    - “Nearness” - new node is physically near

- **Network maintenance** - Establish pairwise keys
  - Send parameters
    - “Nearness” and Privacy
      - Location privacy, Content privacy

Do not Forget: “Nearness” ≠ “Authentication”

(Still, adversaries need to be near their targets 😊)
II. FEASIBILITY

Selecting an “Out-of-Band” Channel for Sensor Networks

• Analysis:
  - Different types of “Out-of-Band” channels
  - HW Requirements

• QUESTIONS:
  - ¿“OUT-OF-BAND” CHANNEL FOR SENSOR NODES?
“Out-of-Band” channels

- **Human users**
  - Read information from sender,
    → input information in receiver
  - Disadvantages:
    • HW Requirements (display, input)
    • Bandwidth is very constrained
  - Simplifications:
    • Single functional buttons
    • Accelerometers - Shaking devices

- **Ultrasound**
  - Advantages
    • Signals stay inside a room (walls)
    • Derive (distance, position) of the sender
“Out-of-Band” channels

- **Visual channel** - Camera
  - Image-based:
    - Data encoded as 2D barcode
    - Receiver (camera) takes a snapshot
  - Light-based:
    - Data encoded as pulses of light
    - Receiver (camera) detect changes

- **Optical channel** - Light
  - Unidirectional
    - Sender: LED
    - Receiver: Photosensor
  - Bidirectional
    - Sender + Receiver: BiDi. LED

Barcode images © shotcode.com, Andrew Currie
LED image © howstuffworks.com
“Out-of-Band” Channels

Feasibility

• **Use light** as a transmission channel (optical channel)
  - Most motes equipped with LED + Photosensor
    • And if not, they are cheap!

• **Aspects to consider:**
  - *Speed*? Limited by the speed of the LEDs / photosensors
  - *Transmission range*? Small (channel noise!)
  - *Activate channel*? Buttons / “Shake” / ...

---

**Fig. 1 — 0603 Ultra Compact**

*Diagrams showing dimensions of components.*

Digikey 404-1017-1-ND

Hamamatsu S1087
III. SECURITY

Security of Optical Channels in Sensor Networks

- Optical channels are “weak”:
  - Easy to eavesdrop / inject messages
    - Light is cheap to produce and sense!
- QUESTION: ¿ARE THEY SECURE ENOUGH?
“Out-of-Band” Channels
Security Analysis

• Light is easy to capture and easy to produce
  - Attacks!
  ✗ **Man-in-the-Middle Attack**
    - Improbable - User Interaction
  ✗ **“Nearness” and Packet Injection**
    - Long-distance communication channels through laser diodes
      • Need to have a lens in the receiver side
    - Use other short-range communication technologies
      • Need unobstructed view between receiver and rogue sender
      • Photosensors that do not sense Infrared light (IrDA)
        - The user can “see” the attack
“Out-of-Band” Channels
Security Analysis

- **Denial of Service attack (DoS)**
  - Modify the ambient light
    - The user can “see” the attack, adaptative sensing
  - “Blind” the photosensor of the receiver
    - The user can “see” the attack + Need of an unobstructed view

- **Eavesdropping**
  - Humans cannot “see” if the channel has enough speed
  - ...but machines can! (Professional digital camcorder: 1000 fps)
  - ...and also specialized equipment can sense it (read info <30 meters)
    - Limit the optical emanations (closed room, covering nodes)
    - Use more than one color to transmit information (optical pass filters)
IV. IMPLEMENTATION

Implementing an Optical Channel in a Mote

- What we need to prove?
  - Feasibility, Speed, Usability
- QUESTION: ¿CAN WE IMPLEMENT A FEASIBLE, FAST, USABLE OPTICAL CHANNEL?
Implementation
Design decisions

Blue LED (0.05 lumens)
(3000 lx. on contact)

1. Blue LED (0.05 lumens)
2. OOK (On-Off Keying), Raw bitrate predefined at design time
3. Dynamically define a threshold during the SYNC block → Adaptative
Implementation
Experiment

1. Human pushes receiver’s button
2. Human pushes sender’s button
3. Information is sent (500bps)
4. Check CRC, LED’s blink
Implementation

Experiment

- **Speed**: 500bps
  - AES-128 key: 0.256 sec.
  - ECC Public key: 0.704 sec.

- **Usability**: 12 tests subjects
  - Arithmetic mean of n# attempts: 2.166
  - Std. Deviation: 0.799

- **Feasibility**
  - Sender: 54B RAM, 1kB ROM
  - Receiver: 126B RAM, 5kB ROM
  - Illuminance conditions: Small transmission range, almost all scenarios

<table>
<thead>
<tr>
<th>Ambient light conditions</th>
<th>Light Intensity</th>
<th>Max. Trans. range</th>
<th>Number of trials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear night</td>
<td>4 lx</td>
<td>6 cm</td>
<td>5 / 5</td>
</tr>
<tr>
<td>Incandescent light</td>
<td>100 lx</td>
<td>3 cm</td>
<td>5 / 5</td>
</tr>
<tr>
<td>Fluorescent light</td>
<td>70-140 lx</td>
<td>3 cm</td>
<td>5 / 5</td>
</tr>
<tr>
<td>Cloudy day</td>
<td>2700 lx</td>
<td>Contact</td>
<td>5 / 5</td>
</tr>
<tr>
<td>Sunlight</td>
<td>3400 lx</td>
<td>Contact</td>
<td>0 / 5</td>
</tr>
</tbody>
</table>
V. CONCLUSIONS

An optical channel for sensor networks
Conclusions

• What are the questions we have answered?
  - “Out-of-band” channels are useful for sensor networks
    • Pre-deployment phase, Network extensibility, Network maintenance
  - Cheap “Out-of-band” channel for motes
    • Optical channel using LEDs and Photosensors
  - Optical channels do provide the necessary security properties
    • Need to take into account the eavesdropping issue
  - The optical channel is feasible, reasonably fast, usable

• What are the questions we have raised?
  - Are the benefits good enough to consider its application outside research environments
  - Is it possible to receive information from *any* light emitting device?
    • Interoperation in Pervasive environments
¡GRACIAS!

Time for Questions 😊